(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年1 月22 日 (22.01.2004)

PCT

(10) 国際公開番号
WO 2004/008684 A1

(51) 国際特許分類[7]: H04L 9/32, G09C 1/00, G06T 7/00

(21) 国際出願番号: PCT/JP2003/008631

(22) 国際出願日: 2003 年7 月7 日 (07.07.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-201444 2002 年7 月10 日 (10.07.2002) JP

(71) 出願人 (米国を除く全ての指定国について): シャープ株式会社 (SHARP KABUSHIKI KAISHA) [JP/JP]; 〒545-8522 大阪府 大阪市 阿倍野区長池町22番22号 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 吉村 秀義 (YOSHIMURA,Hideyoshi) [JP/JP]; 〒639-1007 奈良県 大和郡山市 南郡山町662、663 Nara (JP).

(74) 代理人: 倉内 義朗 (KURAUCHI,Giro); 〒530-0047 大阪府 大阪市 北区西天満４丁目１４番３号住友生命御堂筋ビル Osaka (JP).

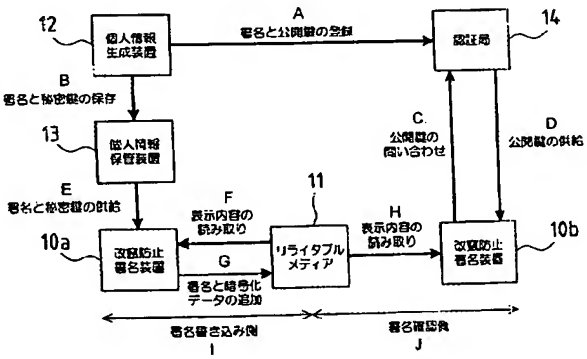
(81) 指定国 (国内): CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

(54) Title: FALSE ALTERATION PREVENTION SIGNATURE METHOD

(54) 発明の名称: 改竄防止署名方法



12...PERSONAL INFORMATION GENERATION DEVICE
A...REGISTER SIGNATURE AND PUBLIC KEY
14...AUTHENTICATION AUTHORITY
B...SAVE SIGNATURE AND PRIVATE KEY
13...PERSONAL INFORMATION STORAGE DEVICE
C...MAKE INQUIRY ABOUT PUBLIC KEY
D...SUPPLY PUBLIC KEY
E...SUPPLY SIGNATURE AND PRIVATE KEY
10a ...FALSE ALTERATION PREVENTION SIGNATURE DEVICE
F...READ DISPLAY CONTENTS
G...ADD SIGNATURE AND ENCRYPTED DATA
11...RE-WRITABLE MEDIUM
H...READ DISPLAY CONTENTS
10b ...FALSE ALTERATION PREVENTION SIGNATURE DEVICE
I...SIGNATURE WRITING SIDE
J...SIGNATURE CONFIRMATION SIDE

(57) Abstract: A false alteration prevention signature device comprises a feature extraction unit (33) that extracts a feature value representing the feature of image data according to an instruction from an authenticator who has authenticated display data; an encryption/decryption unit (35) that encrypts the feature value using an encryption key a paired with an identifier to generate encrypted data, and decrypts the encrypted data into the feature value; a medium writing unit (34) that adds the identifier and the encrypted data to a re-writable medium; and a controller (37) that checks if the decrypted feature value matches the feature value extracted from image data generated by reading display data.

(57) 要約: 本改竄防止署名装置は、表示データを認証した認証者の指示により、画像データの特徴を表す特徴量を抽出する特徴抽出部３３と、識別子と対になった暗号鍵を用いて特徴量を暗号化することにより暗号化データを生成し、かつ、暗号化データを特徴量に復号化する暗号化・復号化部３５と、識別子と暗号化データとをリライタブルメディアに付加するメディア書き込み部３４と、復号化された特徴量と表示データを読み込んで生成した画像データから抽出した特徴量との一致を判定するコントローラ３７とを備えている。

WO 2004/008684 A1

明 細 書

改竄防止署名方法

技術分野

本発明は、表示データの書き込みおよび消去ができるリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。特に、表示データの改竄の防止を行うためのリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

背景技術

従来、契約書等の紙を用いた証明物を扱うときには、証明者がボールペンで署名を行ったり、インクを用いて捺印等を行ったりすることにより、内容を確認したことの証明を行っていた。しかし、このような紙を用いた証明物においては、不要になった場合に、インク等が紙中に浸透しているために文字などを消して紙を再利用することができないといった問題があった。

そこで、近年、資源の有効利用の観点から、紙を用いない証明物の利用が注目されている。紙を用いることなく証明物を作成する際に利用される改竄防止署名システムおよびこのシステムを用いて実施される改竄防止署名方法の一従来例として、例えば、特開平１１－２６１５５０号公報に開示されている電子文書の改竄防止システムおよび方法がある。この電子文書の改竄防止システムおよび方法

において用いられている電子署名技術を用いた署名では、電子データから抽出した特徴量を、秘密鍵を用いて暗号化して電子データに添付して送付するといったものである。そして、電子データ受領者は公開鍵を暗号化された特徴量を用いて復号化し、受け取った電子データの特徴量と復号化した特徴量との一致を確かめることで、受け取った電子データが改竄されていないことを確認している。

また、紙を用いない証明物の一従来例として、特開２０００－３１３１８５号公報に開示されているリライト表示部を有した非接触ＩＣ（集積回路）証明書がある。この非接触ＩＣ証明書はリライタブルメディアのリライト表示部に表示されるものである。このリライタブルメディアとは、電気的、磁気的、または熱的といったような外的要因によって、表示データの内容の書き込みおよび消去が可能なメディアである。このようなリライタブルメディアは、例えば、トナーを含有したマイクロカプセルを用いたメディア、強誘電液晶などの液晶を用いたメディア、およびロイコ染料を用いたメディア等があり、このリライタブルメディアを用いて作成された証明物は再利用が可能である。

しかしながら、前述した電子署名技術においては、証明物が電子文書であることが前提となり、証明を行う際には必ず閲覧用装置が必要であるため、メディア単体で証明が行えないといった問題があった。

一方、前述した非接触ＩＣ証明書を表示するリライタブルメディアにおいては、リライタブルメディア自体が記録された表示データを証明するといった機能を備えたものではないため、証明書発行に煩雑な過程が必要であるといった問題があった。

本発明はこのような問題を解決すべく創案されたものであり、メディア単体で簡単に証明を行うことができるリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

発明の開示

本発明のリライタブルメディアの改竄防止署名方法は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなるといったものである。

本明細書において、特徴量とは、表示データの読み込みデータの特徴を表したものである。例えば、エッジを明確にした表示文字の形状から計算した値や、表示内容を電気的に読み出せるリライタブルメディアにおいては、表示内容そのものから計算して特徴量を得てもよい。

また、暗号化データの記録方法としては、バーコードや、磁性層を設けることで磁気的に記録してもよく、また、ＩＣチップを搭載して記録してもよい。

上記構成において、前記抽出工程が特徴量として表示データを読み込んで生成した画像データから抽出された大まかな特徴を採用する構成であってもよい。

ここで、大まかな特徴とは、画像を折れ線近似した場合の各要素の重心、傾きおよび線の長さ等を示す。

この構成では、照合時に、画像データの読み取り時の揺らぎ等で、現在表示している画像データが暗号化データの画像データと画素単位で完全に一致しない場合でも、特徴量は同一となり一致とみなされ、改竄なしと判断することができる。

本発明の改竄防止署名装置は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実行する改竄防止署名装置であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対にな

った暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えたものである。

本発明の改竄防止署名システムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証する改竄防止署名システムであって、識別子の登録とともに、暗号鍵を生成する暗号鍵生成手段と、識別子と暗号鍵とを保管する保管手段と、識別子による問い合わせにより、暗号鍵を供給する認証手段と、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えてなる改竄防止署名装置とからなるといったものである。

本発明の改竄防止署名プログラムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現するものである。

本発明の改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録

媒体は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現する改竄防止署名プログラムを記録したものである。

上記各発明によれば何れの構成においても、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

図面の簡単な説明

図１は、本発明の改竄防止署名システムの実施の形態を示す説明図である。

図２は、図１に示す改竄防止署名システムに適用されるリライタブルメディアの一例を示す説明図である。

図３は、本発明の改竄防止署名装置の一実施の形態を示す説明図である。

図４は、本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち署名を書き込む手順を示すフローチャートである。

図５は、本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち署名を確認する手順を示すフローチャートである。

図６は、本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち特徴量を抽出する手順を示すフローチャートである。

図７は、図６に示す特徴量を抽出する手順を実施した際に得られる画像データの一例を示す説明図である。

図８は、リライタブルメディアの水平線と読み取りにおける水平線との角度差がある場合の説明図である。

発明を実施するための最良の形態

次に、本発明のリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態について、図面を参照しつつ説明する。

図１は、本発明の改竄防止署名システムの実施の形態を示す説明図である。

この改竄防止署名システムは、暗号鍵生成手段としての個人情報生成装置１２と、保管手段としての個人情報保管装置１３と、認証手段としての認証局１４と、リライタブルメディア１１と、改竄防止署名装置１０ａ，１０ｂとから構成されている。

ここでは、認証者が、署名書き込み側である、図１の左側に図示されている個人情報生成装置１２と個人情報保管装置１３と改竄防止署名装置１０ａとを用いて、リライタブルメディア１１に表示された表示データを認証して署名を行っており、さらに、認証者による署名後、確認者が、署名確認側である、図１の右側に図示されている認証局１４と改竄防止署名装置１０ｂとを用いて、リライタブルメディア１１に表示される表示データが改竄されていないかを確認している。

個人情報生成装置１２は、ユーザが選択した任意の図形データを署名としてデータ化した署名データ（即ち、識別子）２を生成し、この署名データと対になっている、公開鍵暗号方式（例えば１９７７年にマサチューセッツ工科大学のリベ

ストン（Ｒｉｖｅｓｔ）、シャミア（Ｓｈａｍｉｒ）、エーデルマン（Ａｄｌｅｍａｎ）の３人によって発案された公開鍵暗号方式であるＲＳＡ公開鍵暗号方式）による秘密鍵（暗号鍵）および公開鍵（暗号鍵）を生成するものである。

また、個人情報保管装置１３は、例えばフラッシュメモリカード等で構成されており、個人情報生成装置１２によって生成した署名データと秘密鍵とを保存しており、署名データと秘密鍵とを署名書き込み側の改竄防止署名装置１０ａに供給するものである。

さらに、認証局１４は、署名データとその対となっている公開鍵とを保存しており、署名確認側が署名データを用いて問い合わせを行うことにより、改竄防止署名装置１０ｂに対象情報と公開鍵とを供給するものである。

図２は、図１に示す改竄防止署名システムに適用されるリライタブルメディアの一例を示す説明図である。

リライタブルメディア１１は、情報記載域１０９と、複数の署名領域（ここでは、第１承認者の署名領域１０５、第２承認者の署名領域１０６、第３承認者の署名領域１０７および第４承認者の署名領域１０８がある）と、２次元バーコード記載域（ここでは、第１承認者の暗号化データ２次元バーコード記載域１０１、第２承認者の暗号化データ２次元バーコード記載域１０２、第３承認者の暗号化データ２次元バーコード記載域１０３および第４承認者の暗号化データ２次元バーコード記載域１０４がある）とからなり、表示データおよび署名データを記録するものである。さらに、情報記載域１０９には、文書や、図形等の表示データが表示されている。また、第１承認者の署名領域１０５、第２承認者の署名領域１０６、第３承認者の署名領域１０７および第４承認者の署名領域１０８には、表示データを認証した認証者の署名データが記録されている。なお、認証者が複数いる場合は、複数の署名データが各署名領域に一つずつ記載される。さらにまた、第１承認者の暗号化データ２次元バーコード記載域１０１、第２承認者の暗号化データ２次元バーコード記載域１０２、第３承認者の暗号化データ２次元バーコード記載域１０３および第４承認者の暗号化データ２次元バーコード記載域１０４には、認証時の表示データを暗号化した暗号化データがバーコードとして記録されている。なお、記録される位置は、署名された順番に対応して決めら

れている。

図３は、本発明の改竄防止署名装置の一実施の形態を示す説明図である。

改竄防止署名装置１０は、コンソール３６と、改竄判定手段としてのコントローラ３７と、メディア読み取り部３０と、領域認識部３１と、入力補正部３２と、特徴量抽出手段としての特徴抽出部３３と、付加手段としてのメディア書き込み部３４と、暗号化・復号化手段としての暗号化・復号化部３５と、認証局通信装置３８と、個人情報保管装置Ｉ／Ｆ（ｉｎｔｅｒｆａｃｅ）３９とから構成されており、署名データの書き込み、表示データの確認を行うものである。

コンソール３６は、ユーザが指示および選択を行う際や、ユーザにデータを示す際に使用されるものであり、キーボードやモニタ等といった装置を備えている。

コントローラ３７は、汎用のＣＰＵ（ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ）で構成されており、改竄判定手段として機能するのみならず改竄防止署名装置の一連の動作をコントロールするものである。

メディア読み取り部３０は、リライタブルメディア１１の表示面全体を光学的に読み取り、読み取った情報を電気信号に変換するものである。このメディア読み取り部３０は、図示しないＣＣＤ（ｃｈａｒｇｅ　ｃｏｕｐｌｅｄ　ｄｅｖｉｃｅ）ラインイメージセンサユニットと副走査方向駆動系とを備えており、リライタブルメディア１１を走査して、一主走査ライン毎にＲＧＢ（「Ｒ」は「赤」の略であり、「Ｇ」は「緑」の略であり、「Ｂ」は「青」の略である。）カラー信号を生成し、Ａ／Ｄ（ａｎａｌｏｇ　ｔｏ　Ｄｉｇｉｔａｌ）変換により、このＲＧＢカラー信号を有効範囲のみデジタルデータに変換し、領域認識部３１に出力する。

領域認識部３１は、入力データに対して処理を行い、図２に示す署名領域、２次元バーコード記載域およびその他の領域等といった各領域の判別を行い、領域判別後の入力画像データを入力補正部３２に出力するものである。

入力補正部３２は、領域判別後の入力画像データを用いてスキュー補正および倍率補正を行い、入力データを補正し、補正後の入力データを特徴抽出部３３に出力するものである。

特徴抽出部３３は、補正後の入力データに対して、領域認識部３１が判別した領域認識結果に基づいて、署名領域と２次元バーコード記載域とを除いた領域に関して、入力画像データから特徴量を抽出し、抽出した特徴量を示すデータを暗号化・復号化装置３５に出力するものである。

暗号化・復号化装置３５は、コントローラ３７からの指示により、特徴量の暗号化または暗号化データの復号化を行うものである。

メディア書き込み部３４は、署名データおよび２次元バーコード記載域をリライタブルメディア１１に書き込むものである。

認証局通信装置３８は、電話回線またはインターネット通信網等といったネットワーク回線を用いて認証局１４との間で通信を行い、署名データを用いた問い合わせや公開鍵の取得等を行うものである。

個人情報保管装置Ｉ／Ｆ３９は、個人情報保管装置１３とのインタフェースを取りもつものであり、署名データや秘密鍵の取得等を行うものである。

次いで、このような構成を備えた改竄防止署名システムを用いたリライタブルメディアの改竄防止署名方法について説明する。

図４～図６は、本発明のリライタブルメディアの改竄防止署名方法の一実施の形態を示すフローチャートであり、図４は、署名を書き込む手順を示すフローチャートであり、図５は、署名を確認する手順を示すフローチャートであり、図６は、特徴量を抽出する手順を示すフローチャートである。

まず初めに、図４を参照しつつ、認証者が新たな表示データを認証して、新たな署名データをリライタブルメディアに書き込むフローを説明する。

まず、既に書き込まれている署名データがあるか否かを確認し（ステップＳ１）、もし、署名データがある場合（ステップＳ１での判断結果が「はい」である場合）には、署名データが認証局に登録されているか否かを確認する（ステップＳ２）。

もし、署名データが認証局に登録されている場合（ステップＳ２での判断結果が「はい」である場合）には、表示データが改竄されているか否かを確認する（ステップＳ３）。

ここで、署名データが認証局に登録されていない場合（ステップＳ２での判断

結果が「いいえ」である場合）、または署名データが認証局に登録されているが表示データが改竄されていた場合（ステップＳ２およびステップＳ３での判断結果が「はい」である場合）には、新たな第１署名データの書き込みを中止し（ステップＳ４）、処理を終了する。

一方、署名データがない場合（ステップＳ１での判断結果が「いいえ」である場合）、または表示データが改竄されていない場合（ステップＳ３での判断結果が「いいえ」である場合）には、リライタブルメディアの表示面全体を読み取り（ステップＳ５）、さらに、読み取った画像データに関して、２次元バーコード記載域、署名領域および情報記載域それぞれを認識する（ステップＳ６）。

次いで、入力画像がスキューをもっている場合、すなわち図８に示すように、リライタブルメディア１１の水平線と読み取りにおける水平線との角度差がある場合には、そのスキュー角度５０を情報記載域の周辺エッジ角度５１から判別し、そのスキューをアフィン変換で補正する等といった画像補正を実行して表示データを得る（ステップＳ７）。

そして、このような手順によって得られた表示データの特徴を抽出し（ステップＳ８）、さらに、特徴抽出によって得られた符号データ列からＭＤ５（Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ　５　ＲＦＣ１３２１）で１６バイトのハッシュ値を取得することによって特徴量を計算する（ステップＳ９）。

続いて、取得したハッシュ値を、個人情報保管装置から得た秘密鍵を用いて暗号化する（ステップＳ１０）。

最後に、既に書き込まれていた署名データの次の欄に、個人情報保管装置から読み出した新たな署名データを書き込むとともに、暗号化したハッシュ値（新たな暗号化データ）を２次元バーコードに変換して書き込む（ステップＳ１１）。

次に、図５を参照しつつ、署名後の新たな表示データに関して改竄の有無を確認する手順、即ち、新たな表示データと現在表示されている表示データとが同一の表示データであるか否かを確認するフローを説明する。

まず、リライタブルメディアの表示面全体を読み取り（ステップＳ２１）、さらに、読み取った画像データに関して、２次元バーコード記載域、署名領域および情報記載域それぞれを認識する（ステップＳ２２）。

次いで、入力画像がスキューをもっている場合には、そのスキュー角度を情報記載域の周辺エッジ角度から判別し、そのスキューをアフィン変換で補正する等といった画像補正を実行して表示データを得る（ステップＳ２３）。

このような手順を実行することによって、リライタブルメディアから、情報記載域に現在表示されている表示データと署名データとを得る。

続いて、既に書き込まれている全ての署名データの中で、確認が終了していないものがあるか否かを判断し（ステップＳ２４）、もし、確認が終了していないものがある場合（ステップＳ２４での判断結果が「いいえ」である場合）には、ステップＳ２５に進み、もし、確認が終了していないものがない場合（ステップＳ２４での判断結果が「はい」である場合）には処理を終了する。

ステップＳ２５では、署名領域の最後に記載された署名データを認証局に送信して、照会を行う。例えば、第１署名領域から第３署名領域までに署名データが記載されているときには、第３署名領域に記載されている新たな署名データを認証局に送信して、照会を行う。

そして、例えば、新たな署名データの読み取りを失敗していた等といった理由等によって、認証局にこの新たな署名データが登録されていないと判断された場合（ステップＳ２６での判断結果が「いいえ」である場合）には、照会ができないので、その旨をユーザに警告通知して（ステップＳ２７）、処理を終了する。

一方、新たな署名データが認証局に登録されていた場合（ステップＳ２６での判断結果が「はい」である場合）には、認証局から新たな署名データに対応する登録者情報と公開鍵とを受け取るとともに、リライタブルメディアから新たな署名データに対応する２次元バーコード記載域から２次バーコードを読み取り、暗号化データを得る（ステップＳ２８）。

続いて、暗号化データを公開鍵を用いて復号化して、認証された表示データの特徴量を得る（ステップＳ２９）。そして、前述したステップＳ２１で読み取ったリライタブルメディアの情報記載域に表示されている表示データから特徴量を抽出し（ステップＳ３０）、特徴量を計算する（ステップＳ３１）。

その後、情報記載域に表示されている特徴量と認証された特徴量とを比較して（ステップＳ３２）、情報記載域に表示されている特徴量と認証された特徴量と

が一致しているか否かを判定する（ステップＳ３３）。

もし、一致している場合（ステップＳ３３での判断結果が「はい」である場合）には、処理の対象となっている署名データについて、書き込み時からの改竄はないとみなし、ステップＳ２４に戻り、残りの署名データに関して、照会と特徴量の比較と（ステップＳ２４～ステップＳ３３）を署名データの数だけ繰り返し実行する。そして、全ての署名データに関して処理を終了したときには、ステップＳ２４で確認終了したと判断されるので（ステップＳ２４での判断結果が「はい」になるので）、処理を終了する。

一方、ステップＳ３３において一致していないと判断された場合（ステップＳ33での判断結果が「いいえ」である場合）には、処理の対象となっている署名データについて、書き込み後に改竄がなされたとみなし、コンソールを通じてユーザに対して警告通知を行い（ステップＳ２７）、処理を終了する。

次に、改竄防止署名装置を構成する特徴抽出部の動作について、図６を参照しつつ説明する。

ここでは、リライタブルメディアの表示が電子的に読み出せない場合を例に挙げて説明する。

表示データの読み込み時には、例えば図７（ａ）に示すような画像データ（太線の「Ａ」）４１が読み込まれるので、この画像データを用いてエッジ抽出する。このエッジ抽出では、まず、対象画素Ｐ１（ｘ，ｙ）の画素濃度を表す画素値ｐ１（ｘ，ｙ）から、対象画像Ｐ１の左の画素Ｐ２の画素値ｐ２（ｘ－１，ｙ）を減算し、減算によって得られた値の絶対値が閾値（Ｔｅｄｇｅ）以上であれば、対象画素Ｐ１がエッジ画素であると判定する。そして、処理の対象となっている画像データを構成する全ての画素について、エッジ画素とそれ以外の画素とで２値化する。その後、画像データの左上から順に全ての画素について水平方向および垂直方向の順に走査し、検出したエッジ画素を基点として画像データ中のエッジ画素で囲まれた領域の輪郭線追跡を行う（ステップＳ４１）。その結果、例えば、図７（ｂ）に示すような輪郭線データ４２を得る。

続いて、輪郭線データを参照して、輪郭線で囲まれた領域について細線化処理を行い（ステップＳ４２）、その結果、例えば、図７（ｃ）に示すような細線４

3を得る。その後、得られた細線を直線化して折れ線近似し（ステップＳ４３）、その結果、例えば、図７（ｄ）に示すような近似画像４４を得る。

次いで、得られた近似画像を参照して、画像データの左上から全ての画素について順に水平方向および垂直方向の順に走査し、折れ線の重心点を発見した順に折れ線をナンバリングする。さらに、ナンバリングされた折れ線の順に、折れ線重心点（ｘｉ，ｙｉ）、折れ線長Ｌｉ、折れ線の水平からの角度θｉのそれぞれのパラメータを抽出する（ステップＳ４４）。

最後に、抽出したパラメータをそれぞれ量子化し、さらに、量子化した各値をナンバリングの順に連結して符号データ列を作成する（ステップＳ４５）。この際に、読み取り時の誤差を考慮して、読み取り時に判別が可能なパラメータのみを結合することが好ましい。

また、前述した手順、即ち、リライタブルメディアの改竄防止署名方法は改竄防止署名プログラムによって実現される。さらに、改竄防止署名装置のコントローラ３７には、この改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体が含まれている。この記録媒体としては、マスクＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）およびフラッシュＲＯＭといった半導体記憶素子、ハードディスク、フレキシブルディスク、ＭＯ（Ｍａｇｎｅｔｏ－Ｏｐｔｉｃ）ディスク、ＣＤ（Ｃｏｍｐａｃｔ Ｄｉｓｃ）－ＲＯＭ、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）－ＲＯＭ、光磁気ディスク、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）カード、および磁気テープ等をあげることができ、プログラムを記憶することが可能であれば、他の記録媒体であってもよい。また、プログラムそのものを通信により伝送して記録媒体に記録するといったものであってもよい。

以上のように、本実施の形態のリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体によれば、表示データに暗号化された特徴量と、その識別子とが付加されるので、リライタブルメディア単体で、表示データに改竄があるかどうかを簡単に判別することができる。

また、表示内容を大まかに抽出して、エッジが明確な文字の形状情報など、情報の本質から特徴量を抽出するので、例えば、リライタブルメディアの表示内容を複写機でコピーして得られた複写物においても、署名データの有効性を確認することができる。

さらにまた、リライタブルメディアが表示内容読み出し機能を備えており、電子的に表示データを値として読み出すことが可能なメディアである場合、またはエラー訂正技術等によって、読み出しエラー率が充分に低いリライタブルメディアと改竄防止署名装置とを用いている場合においては、表示データの読み取りデータ列を連結したものを符号データ列として用いてもよい。この場合には、前述した手順を実施すると、表示内容そのものから特徴量を抽出しているので、表示データが署名時と完全に同じであることを確認することができる。

一方、リライタブルメディア上での暗号化データの記録手段は、２次元バーコードに限定されず、磁性層を設けることで磁気的に記録してもよく、また、ＩＣチップを搭載することで、ＩＣチップに表示データを電子化したデータと暗号化データとを同時に記録するようにしてもよい。

なお、リライタブルメディア上の各領域（署名領域、２次バーコード記載域および情報記載域）は位置を固定化しなくてもよい。このように、位置を固定化しない場合には、領域判別によって各領域に分離して処理を進めることができる。また、署名データに関しては、類推されるものをすべて認証局に問い合わせることで判別すればよい。

産業上の利用可能性

本発明は、認証時及び認証後の表示データの読み取りの際、揺らぎ等により両者の読み取りデータに不一致の要素が含まれていたとしても、本発明では読み込んだ表示データの特徴量をそれぞれ抽出し、その両者の抽出特徴量に基づいて比較するようにしたので、常に正確に表示データの改竄の有無を判別することができる点で有益であり、改竄防止に優れた効果が期待できる。

請 求 の 範 囲

1． 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法であって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、

これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、

認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程と

からなることを特徴とするリライタブルメディアの改竄防止署名方法。

2． 前記抽出工程において、表示データを読み込んで生成した画像データから抽出された大まかな特徴を特徴量として採用する請求の範囲第1項に記載のリライタブルメディアの改竄防止署名方法。

3． 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実行する改竄防止署名装置であって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、

1識別子と暗号化データとをリライタブルメディアに付加する付加手段と、

復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段と

を備えたことを特徴とする改竄防止署名装置。

4. 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証する改竄防止署名システムであって、

識別子の登録とともに、暗号鍵を生成する暗号鍵生成手段と、

識別子と暗号鍵とを保管する保管手段と、

識別子による問い合わせにより、暗号鍵を供給する認証手段と、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えてなる改竄防止署名装置と

からなることを特徴とする改竄防止署名システム。

5. 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、

これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、

認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程と

からなることを特徴とする改竄防止署名方法を実現するための改竄防止署名プログラム。

6． 請求の範囲第５項に記載の改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体。

図1

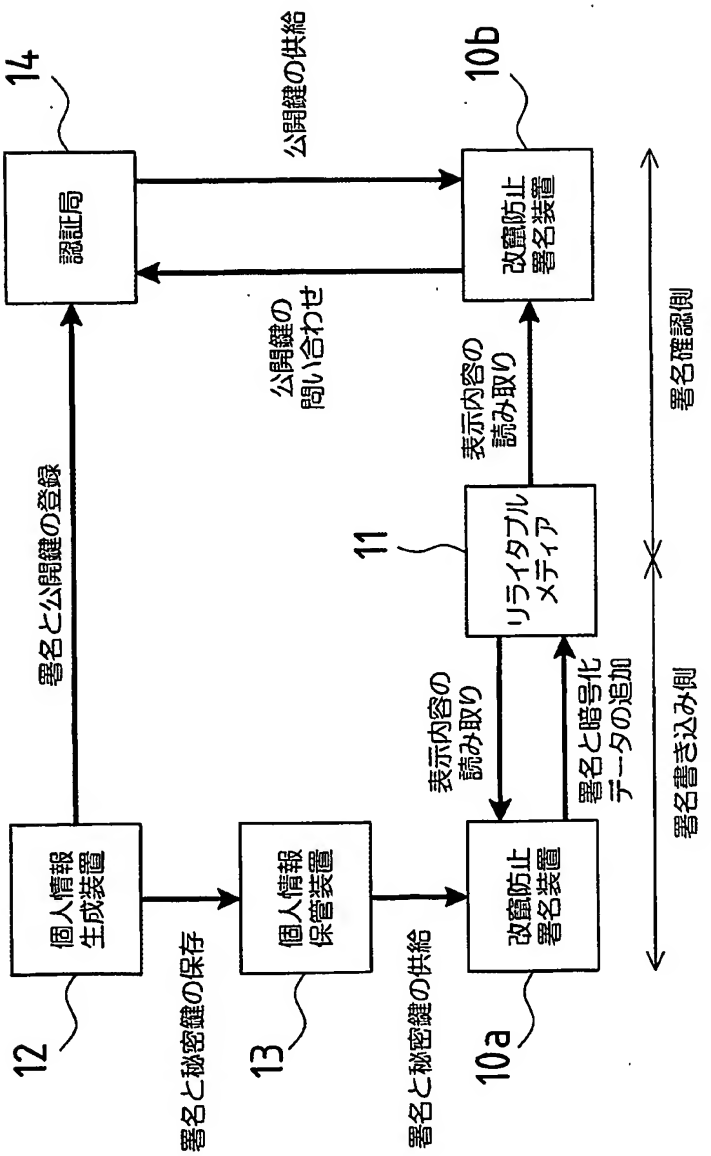

14
認証局
公開鍵の供給
10b
改竄防止
署名装置
公開鍵の
問い合わせ
署名と公開鍵の登録
表示内容の
読み取り
11
リライタブル
メディア
署名確認側
表示内容の
読み取り
署名と暗号化
データの追加
署名書き込み側
12
個人情報
生成装置
署名と秘密鍵の保存
13
個人情報
保管装置
署名と秘密鍵の供給
10a
改竄防止
署名装置

図2

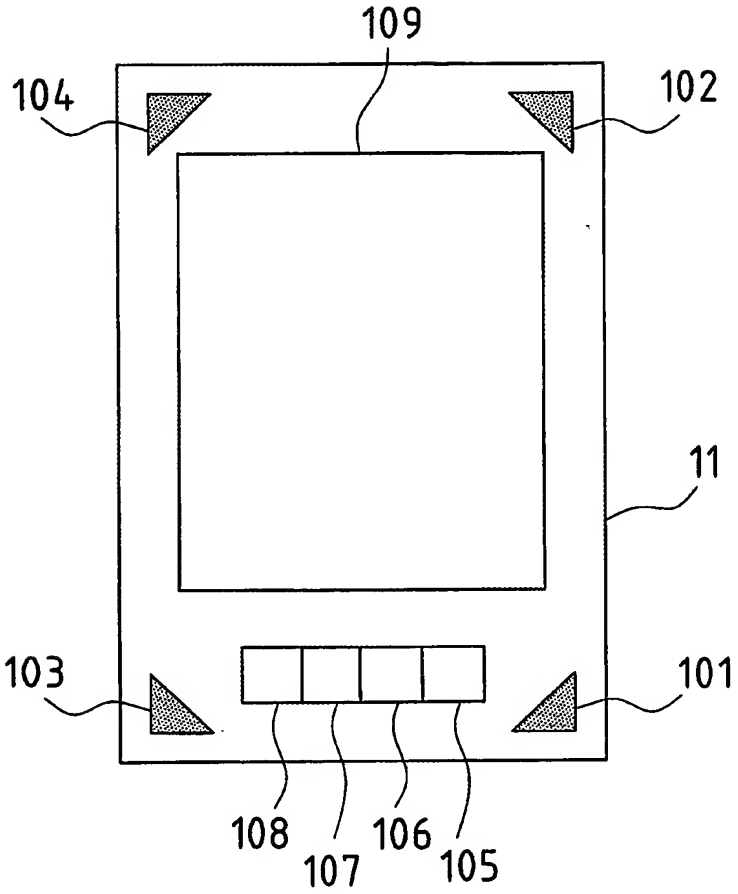


図3

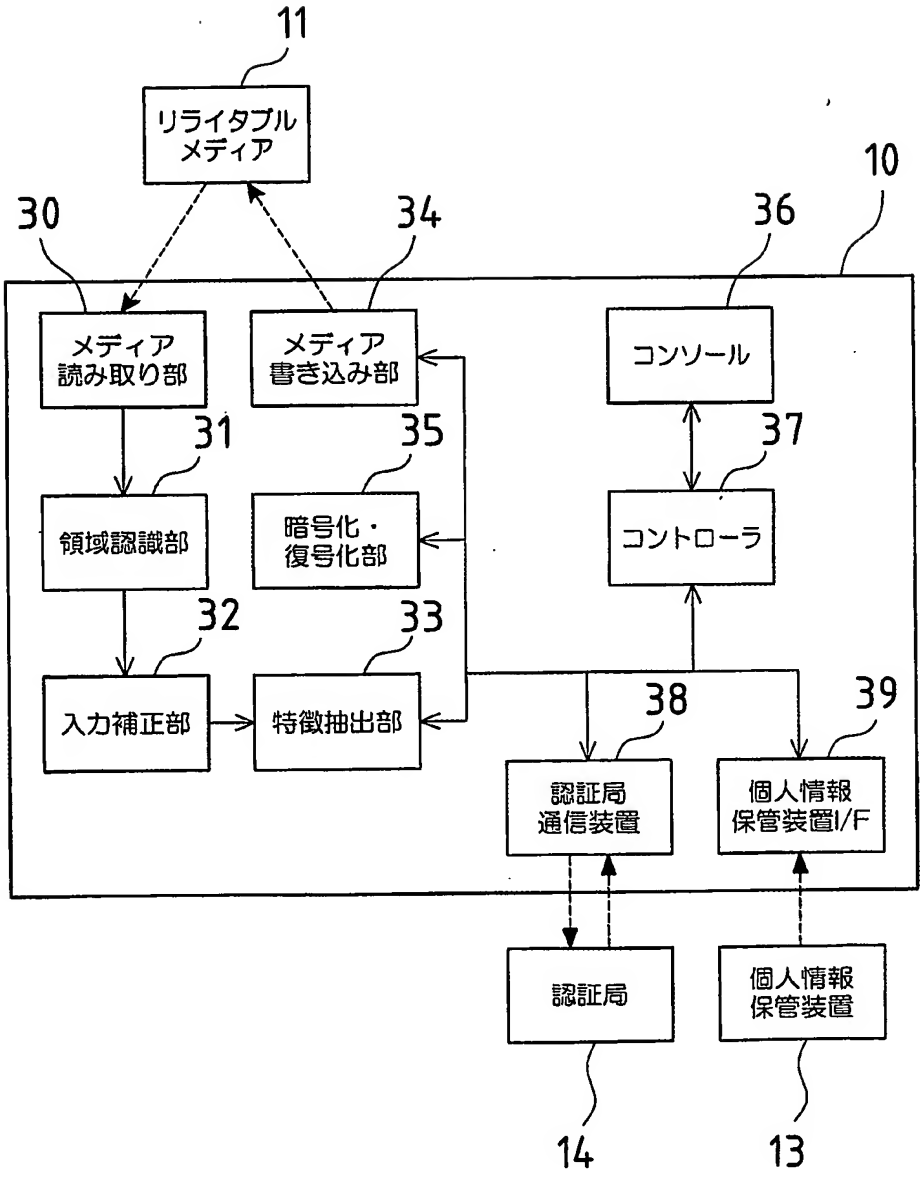

11
リライタブル
メディア
10
30
34
36
メディア
読み取り部
メディア
書き込み部
コンソール
31
35
37
領域認識部
暗号化・
復号化部
コントローラ
32
33
38
39
入力補正部
特徴抽出部
認証局
通信装置
個人情報
保管装置I/F
認証局
個人情報
保管装置
14
13

図4

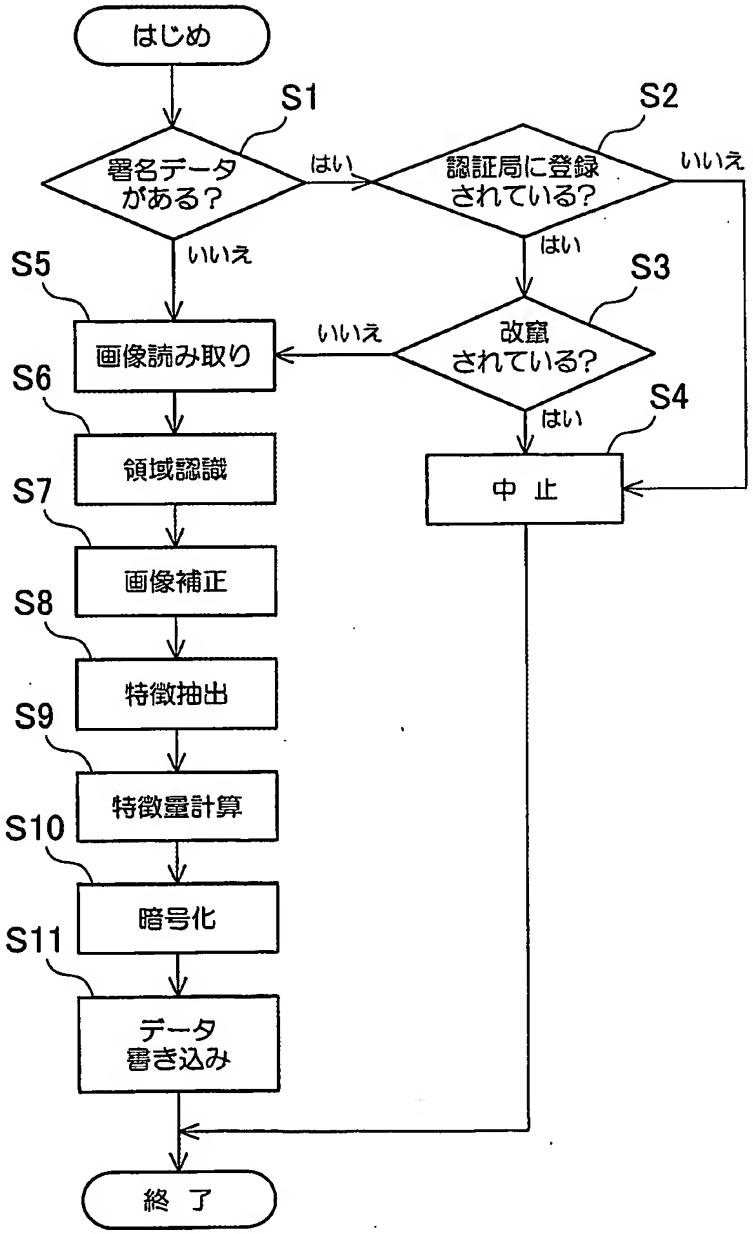

はじめ
S1
署名データがある？
はい
S2
認証局に登録されている?
いいえ
いいえ
はい
S5
S3
画像読み取り
いいえ
改竄されている?
S6
はい
S4
領域認識
中 止
S7
画像補正
S8
特徴抽出
S9
特徴量計算
S10
暗号化
S11
データ書き込み
終 了

図5

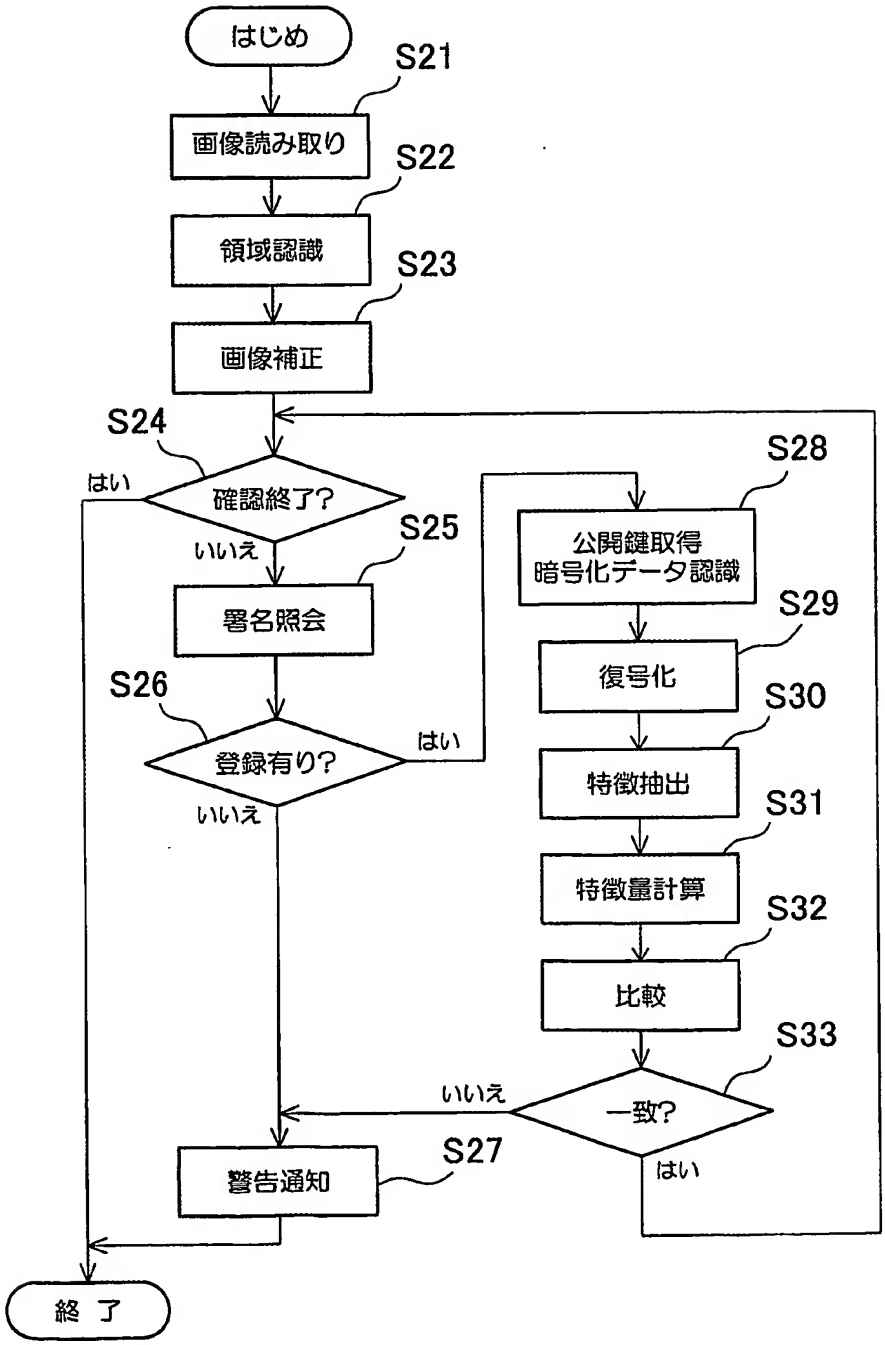

はじめ
S21
画像読み取り
S22
領域認識
S23
画像補正
S24
確認終了?
はい
いいえ
S25
署名照会
S26
登録有り?
はい
いいえ
S27
警告通知
終了
S28
公開鍵取得
暗号化データ認識
S29
復号化
S30
特徴抽出
S31
特徴量計算
S32
比較
S33
一致?
いいえ
はい

図6

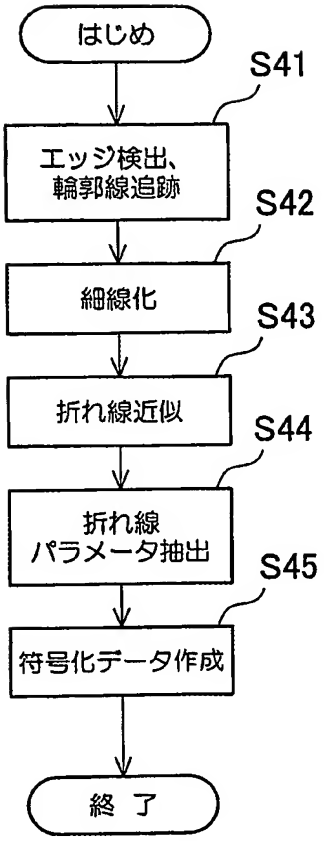
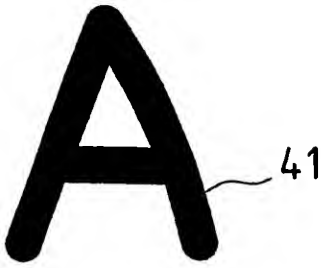
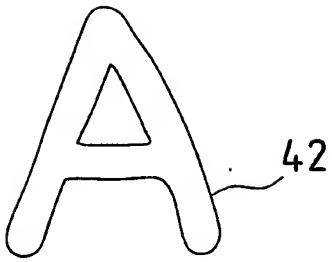

はじめ
S41
エッジ検出、
輪郭線追跡
S42
細線化
S43
折れ線近似
S44
折れ線
パラメータ抽出
S45
符号化データ作成
終 了

図7

(a)



(b)



(c)

(d)

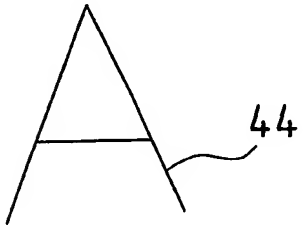


図8